

## ABSTRACT

The method of the invention is implemented in a communication network comprising a source device (1) that contains:

- 5                   - a first symmetric key ( $K_C$ ) for encrypting the data (CW) to be sent to a presentation device (2) connected to the network; and
- said first symmetric key ( $K_C$ ) encrypted ( $E2\{K_N\}(K_C)$ ) with a second symmetric network key ( $K_N$ ) known only by at least one presentation device (2) connected to the network.

10                  When the source device needs to renew its first symmetric key ( $K_C$ ) to encrypt new data, it generates a random number (D), then calculates a new symmetric key ( $K'_C$ ) based on the first symmetric key ( $K_C$ ) and on the random number (D). It then encrypts the data to be transmitted (CW) with the new symmetric key ( $K'_C$ ) then it transmits to a presentation device, via the network:

- 15               - the data encrypted with the new symmetric key ( $E3\{K'_C\}(CW)$ );
- the random number (D); and
- the first symmetric key encrypted with the second symmetric network key ( $E2\{K_N\}(K_C)$ ).

20

Figure 3.